Ontario Tumour Bank

# Submission to the Information and Privacy Commissioner Ontario in Respect of the Ontario Tumour Bank's Status as a Prescribed Person under Section 39(1)(c) of the *Personal Health Information Protection Act, 2004*

## 2023 Submission

OICR
Ontario Institute
for Cancer Research

## Contents

BACKGROUND INFORMATION ........ 3

Introduction ........ 3

Background ........ 3

Definitions ........ 4

Privacy, Security and Other Indicators ........ 6

Part 1 – Privacy Indicators ........ 6

Part 2 – Security Indicators ........ 25

Part 3 – Human Resources Indicators ........ 32

Part 4 – Organizational Indicators ........ 38

Appendix A: Privacy Recommendations from the OTB's annual Freezer and Operational Audit ........ 40

Appendix B: Ontario Tumour Bank Security IT Audit Summary ........ 41

Appendix C: OICR Policy Reviews and Amendments ........ 45

Appendix D: OTB Privacy Checklist ........ 58

# BACKGROUND INFORMATION

## Introduction

The Ontario Tumour Bank (OTB) is a province-wide biorepository and data bank focused on collection of tumour-related human biospecimens. It provides academic and industry cancer researchers with a diverse selection of high quality tumour-related specimens and data obtained directly by dedicated tumour bank staff, who follow a stringent set of procedures and ethical guidelines.

The biospecimens and clinical data are an important resource for scientists engaged in translational research who are developing better diagnostic tools and new drug therapies. Researchers depend on the OTB to provide research biospecimens of high quality, diversity and integrity.

Operating at state-of-the-art hospitals and cancer centres across Ontario, the OTB coordinates the collection, storage, analysis, annotation, and distribution of tumour and peripheral blood samples. Working in collaboration with local pathologists, medical oncologists, surgeons and other hospital personnel, specially trained staff obtain patient consent, collect tissues and assemble comprehensive clinical information about each donor and the corresponding samples.

OTB is a program of the Ontario Institute for Cancer Research (OICR). Funded by the Government of Ontario, OICR is a not-for-profit corporation that supports research on the prevention, early detection, diagnosis, treatment and control of cancer.

The following submission is being provided pursuant to the 2023 Review Cycle as contemplated by the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* in order to obtain continued approval for OICR to maintain its Prescribed Person status in respect of OTB.

## Background

OTB was established in 2004, to respond to a growing need for a provincial tissue and health data bank to support cancer research. OTB is a multi-centred program that collects blood and tissue samples as well as personal health information (PHI) from consenting research participants who have agreed to participate in the OTB. OTB is a source of high quality tumour-related bio-specimens and data for academic and industry-based researchers to conduct cancer research. The outcomes of the research studies are expected to contribute to the provision of health care for cancer patients by providing information that may lead to an increased understanding of the disease and the development of new diagnostic tools and therapies.

OTB has dedicated staff at four hospital-based Collection Centres across Ontario (see Ontario Tumour Bank highlights, below). At each Collection Centre, OTB provides a Principal Investigator with operating funds and establishes contractual obligations for funded staff to execute a common set of standard operating procedures. Each Collection Centre has a local management committee, a clinical research coordinator, and a pathologists' assistant.

OICR was established as a prescribed person under the *Personal Health Information Protection Act, 2004* ("PHIPA" or the "Act") for its activities associated with OTB. As a Prescribed Person, OICR in respect of

OTB, has particular rights and obligations under the Act which apply to its collection, use, and disclosure of PHI for the purposes of compiling and maintaining a registry for the storage of donated tissues. Every three years, OICR in respect of OTB, makes this submission to the Information and Privacy Commissioner/Ontario for their review. Any recommendations stemming from such review are considered and implemented by OICR.

Data collected by OTB Collection Centre staff includes sample data (e.g., sample details) and clinical data (e.g., demographics, diagnosis, stage, treatments, patient history, outcome details). Data is stored and managed in an application called TissueMetrix 2, an integrated web application with a central database located at OICR's premises in Toronto.

Ontario Tumour Bank highlights:

- Ontario-wide biorepository and data bank, collecting blood and tissue samples;
- Four academic teaching hospitals participate as Collection Centres:
    - Kingston General Hospital (sample storage only, no active patient accrual),
    - London Health Sciences Centre,
    - St. Joseph's Healthcare Hamilton, and,
    - The Ottawa Hospital;
- Dedicated staff at each Collection Centre collect samples and clinical data from participating consented donors;
- Stringent procedures and ethical guidelines;
- Samples consented for a wide range of uses, including the development of commercial products;
- OTB makes no claims to intellectual property developed by the recipient of the material; and
- Is a resource for academic and industry researchers: OTB dispenses samples and discloses de-identified data to qualified recipients under a Material Transfer Agreement.

The table immediately below sets out the shortform definitions used in this submission.

## Definitions

| Acronym | Definition |
|---|---|
| KGH | Kingston General Hospital |
| IGC | Information Governance Committee |
| IPC | Information and Privacy Commissioner/Ontario |
| ISO | Information Security Officer |
| LHSC | London Health Sciences Centre |
| MTA | Material Transfer Agreement |

| | |
|---|---|
| OICR | Ontario Institute for Cancer Research |
| OTB | Ontario Tumour Bank |
| PIA | Privacy Impact Assessment |
| PHI | Personal Health Information |
| PHIPA | Personal Health Information Protection Act |
| PO | Privacy Officer |
| SJHH | St. Joseph's Healthcare Hamilton |
| SOP | Standard Operating Procedure |
| TOH | The Ottawa Hospital |
| VPN | Virtual Private Network |

# Privacy, Security and Other Indicators

## Part 1 – Privacy Indicators

| Categories | Privacy Indicators | OICR |
|---|---|---|
| General Privacy Policies, Procedures and Practices | The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario. | **<u>OICR Policies</u>: See Appendix C**<br>**<u>OTB Policies</u>:**<br>Any changes are communicated in three ways each time: (1) verbal communication that modified policies are being shipped (via teleconference), (2) a physical mail-out of the modified documents along with a table of changes and instructions for removing old policies and inserting the new policies into the policy binder, and (3) the policies are changed on the OTB online "collaboration" website. Agents affected by the policies are further instructed to read the modified policies and log this on their training log.<br>**OTB.POL801 – Ontario Tumour Bank Privacy Policy**<br>1) Reviewed on July 22, 2020 (no change).<br>2) Reviewed and amended on September 3, 2021 (major change):<br>a. Changed "blood and tissue samples" in Section 1.0 to "biospecimens"<br>b. Clarified Section 4.3 to state that donors aged 18 years can provide informed consent, the prior version stated "over 18 years" which was inconsistent with informed consent form<br>c. Modified Section 4.3 to have more inclusive language: using "their" instead of "his/her"<br>d. Added additional language to Section 4.5: "provide evidence of compliance with ethics standards or regulation (as relevant to their jurisdiction)" and "for the purposes of subsection 39(1)(c) of the Act" in reference to Personal Health Information Protection Act |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | | e. Deleted reference to Cancer Care Ontario (CCO) from Section 4.5<br>f. Added the language "OICR in respect of" to Section 4.8<br>g. Created Section 6.0: "List of Data Holdings"<br>h. Listed "OTB TissueMetrix database" as a data holding under Section 6.0<br>i. Performed grammatical and formatting revisions<br>Implemented and communicated on December 9, 2021<br>**OTB.POL802 – Policy and Procedures for the Collection of Personal Health Information – Ontario Tumour Bank**<br>1) Reviewed on July 22, 2020 (no change)<br>2) Reviewed on September 4, 2021 (no change)<br>**OTB.POL803 – Policy and Procedures for Data Access and Use – Ontario Tumour Bank**<br>1) Reviewed on July 22, 2020 (no change)<br>2) Reviewed and amended on July 22, 2021 (minor change):<br>a. Clarifying language added to Section 5.2 regarding responsibility for providing notice when terminating agent access<br>Implemented and communicated on December 9, 2021<br>**OTB.POL804 – Policy and Procedures for Data Disclosure – Ontario Tumour Bank**<br>1) Reviewed on July 22, 2020 (no change).<br>2) Reviewed and amended on July 29, 2021 (minor change):<br>a. The acronym "DM" referring to the document management system was changed to "SharePoint" as this is OTB's current document management system<br>b. "Full postal code" was removed from the list of de-identified data released to researchers and moved to the list of direct identifiers that will always be removed to be consistent with other SOPs and practice (this update corrected an inaccuracy of wording in this policy only, confirming that postal |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  |  | code has never been included with the "de-identified" data released to researchers).<br>Implemented and communicated on December 9, 2021<br>**OTB.POL805 – Policy and Procedures for Data Linkages – Ontario Tumour Bank**<br>1) Reviewed on July 22, 2020 (no change)<br>2) Reviewed on April 21, 2021 (no change)<br>**OTB.POL806 – Business Continuity Plan – Ontario Tumour Bank**<br>1) Reviewed on July 22, 2020 (no change)<br>2) Reviewed on November 12, 2021 (minor change):<br>a. Updated title of executive representative<br>b. Updated title of communications representative<br>c. Deleted "Senior" from OTB Analyst and OTB Client Coordinator role<br>Implemented and communicated on December 9, 2021<br>**TB312 – Material and Data Request and Release**<br>1) Reviewed on July 16, 2020 (no change).<br>2) Reviewed and amended on November 11, 2021 (minor change):<br>a. Added "Tissue Portal at OICR" to Section 4 and changed "Research Technician" to "OTB Research Technician"<br>b. Added "Referrals from the Provincial PI or the OTB Director" to Section 6.1<br>c. Added the use of OICR Transfer, an encrypted file transfer service, for preliminary data report (aka sample search report) to Section 6.2.4<br>d. Added Section 6.3 "Creating a Requisition" to provide direction on how this should be done within the Biobanking Information Management System.<br>e. Deleted "Senior" from Client Coordinator role<br>Implemented and communicated on December 9, 2021 |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | | **DM502 – Tissue Metrix Access and Configuration**<br>1) Reviewed and amended on July 20, 2020 (minor change):<br>a. Changed TissueMetrix to TissueMetrix2<br>b. Added instructions on password retrieval to Section 6.2.2<br>c. Added to Section 6.3: "In the event of a patch upgrade to the TissueMetrix2 system or database, the Tumour Bank Analyst will perform user acceptance testing (UAT) on TissueMetrix2"<br>Implemented and communicated on December 17, 2021<br>**TB311 – Physical Security of OTB Facilities**<br>1) Reviewed on July 2, 2020 (no change)<br>2) Reviewed on June 10, 2021 (no change) |
| | Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made | Amended privacy policies and procedures: see directly above for OTB policies and Appendix C for OICR policies |
| | Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of | Newly developed privacy policies and procedures:<br>**TB320 – Remote Work**<br>This procedure describes the principles of remote work for OTB staff. It includes: preparation that must be considered in advance of engaging in remote work; prioritization of work; options for remote meetings; and the procedure for supporting remote audits. |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | the policies and procedures developed and implemented. | Implemented on August 11, 2021. |
| | The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication. | **TB320 – Remote Work**<br>Communicated on August 11, 2021 via email.<br>Amended privacy policies and procedures: see on page 69 for OTB policies and Appendix C for OICR policies. |
| | Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments | The OTB Privacy Policy (amended as indicated on page 9) and the OICR Privacy Policy, were communicated to the public on the OTB or OICR (as applicable) website immediately following the effective date. |
| Collection | The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity. | One data holding containing PHI (TissueMetrix 2). |
| | The number of statements of purpose developed for data | One statement of purpose: |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | holdings containing personal health information | http://www.ontariotumourbank.ca/patients/statement-purpose |
| | The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the Information and Privacy Commissioner of Ontario | One statement of purpose was reviewed (see statement above). |
| | Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made. | None |
| Use | The number of agents granted approval to access and use personal health information for purposes other than research. | 9 – Collection Centre staff<br>8 – OICR staff<br>4 – Inspirata Canada staff (vendor of TissueMetrix 2) |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| | The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| Disclosure | The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| | The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | since the prior review by the Information and Privacy Commissioner of Ontario. |  |
|  | The number of requests received for the disclosure of personal health information for research purposes since the prior review by the Information and Privacy Commissioner of Ontario. | None |
|  | The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the Information and Privacy Commissioner of Ontario. | None |
|  | The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the Information and Privacy Commissioner of Ontario. | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario. | Aggregate inventory reports were provided to Collection Centres on a monthly basis during active accrual (18 reports sent via email from November 1, 2019 – July 31, 2021; 2 reports were not sent out due to staffing absence in November and December 2019).<br>Number of requests for de-identified data sets for researchers:<br>254 (November 1, 2019 – August 2, 2022).<br>Number of requests for the disclosure of de-identified and/or aggregate information for other purposes: 0 (November 1, 2019 – August 2, 2022). |
| | The number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since the prior review by the Information and Privacy Commissioner of Ontario. | Number of Material Transfer Agreements signed and fulfilled:<br>31 (November 1, 2019 – August 2, 2022)<br>+2 Pending MTAs to be signed and executed, +3 MTAs were unfulfilled<br>Unfulfilled MTAs are due to the clients wishing to either no longer move forward with their transaction or have not yet agreed to move forward with their transactions. OTB does not release de-identified data without a signed MTA.  Per OTB procedures (see SOP TB312 sec. 6.2), a preliminary data report (see F-TB312-07) may be shared without an MTA to help potential researchers in the selection of appropriate cases for their study. |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| Data Sharing Agreements | The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. | There have been zero such agreements executed since the prior IPC review, but there are 4 data sharing agreements (one for each Collection Centre) in effect. |
| | The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| Agreements with Third Party Service Providers | The number of agreements executed with third party service providers with access to personal health information since the prior review by the Information and Privacy Commissioner of Ontario. | There have been zero such agreements executed since the prior IPC review, but one agreement, which is with Inspirata Canada, is in effect. It was amended on April 2, 2022 and will be terminated on March 31, 2023. |
| Data Linkage | The number and a list of data linkages of PHI approved since the prior review by the | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | Information and Privacy Commissioner of Ontario. |  |
| Privacy Impact Assessments | The number and a list of privacy impact assessments completed since the prior review by the Information and Privacy Commissioner of Ontario and for each privacy impact assessment:<br>– The data holding, information system, technology or program,<br>– The date of completion of the privacy impact assessment,<br>– A brief description of each recommendation,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | The number and a list of privacy impact assessments undertaken but not completed since the prior review by the Information and Privacy Commissioner and the proposed date of completion. | None |
|  | The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion. | None |
|  | The number of determinations made since the prior review by the Information and Privacy Commissioner of Ontario that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination. | None |
|  | The number and a list of privacy impact assessments reviewed | One. No amendments were made. |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | since the prior review by the Information and Privacy Commissioner and a brief description of any amendments made. |  |
| Privacy Audit Program | The dates of audits of agents granted approval to access and use personal health information since the prior review by the Information and Privacy Commissioner of Ontario and for each audit conducted:<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | See "Security Audit Program" indicator on page Security Audit Program27 below for details. Privacy and Security parameters are audited together in a single audit. |
|  | The number and a list of all other privacy audits completed since the prior review by the | Freezer and Operational Audit is performed on an annual basis which includes review of a Privacy Checklist (see audit recommendations details in Appendix A). The Annual Freezer and Operational Audit is one audit which encompasses storage of samples, general operations, and |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | Information and Privacy Commissioner of<br>Ontario and for each audit:<br>– A description of the nature and type of audit conducted,<br>– The date of completion of the audit,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | privacy and information security items. The excerpt provided in Appendix D, the OTB Privacy Checklist, is the portion of the audit checklist relevant to privacy and information security.<br>11 Annual Freezer and Operational Audits completed since the prior review (conducted at each Collection Centre and at OICR):<br>● February 20, 2020 – TOH<br>● February 24, 2020 – LHSC<br>● February 25, 2020 – SJH<br>● February 27, 2020 – KGH<br>● March 25, 2021 – OICR<br>● March 26, 2021 – LHSC<br>● March 29, 2021 – SJH<br>● February 17, 2022 – LHSC<br>● February 24, 2022 – SJH<br>● February 25, 2022 – KGH<br>● March 25, 2022 – OICR<br>Notes:<br>On-site access and active staff are required for these audits.<br>In 2020, OICR was due for audit in March. However, on-site access was not allowed due to COVID-19.<br>In 2021, there was no audit conducted at TOH or KGH as staff at these institutions resigned and were not replaced.  There was no access to data at these sites.<br>In 2022, no audit was conducted at TOH as staff had not been replaced since their resignation in 2021. There was no access to data at the site. |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | | Annual Privacy Training (no recommendations made) – a review of the OTB Log of Privacy Information Security Training; confirmation of training attestations; and annual renewal of training for OTB agents at OICR and the Collection Centres:<br>• December 2019<br>• January 2021<br>• January 2022<br>Confidentiality Agreement (no recommendations made) – a review of the OTB Log of Executed Confidentiality Agreements; and annual renewal of training for OTB agents at OICR and the Collection Centres:<br>• December 2019<br>• January 2021<br>• January 2022 |
| Privacy Breaches | The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| | With respect to each privacy breach or suspected privacy breach: | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | – The date that the notification was received,<br>– The extent of the privacy breach or suspected privacy breach,<br>– Whether it was internal or external,<br>– The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations, |  |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | – The date that the investigation was commenced,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | |
| Privacy Complaints | The number of privacy complaints received since the prior review by the Information and Privacy Commissioner of Ontario. | None |
| | Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the Information and Privacy | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | Commissioner of Ontario and with respect to each privacy complaint investigated:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint,<br>– The date that the investigation was commenced,<br>– The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, |  |

| Categories | Privacy Indicators | OICR |
|---|---|---|
| | – The manner in which each recommendation was addressed or is proposed to be addressed, and<br>– The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint. | |
| | Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the Information and Privacy Commissioner of Ontario and with respect to each privacy complaint not investigated:<br>– The date that the privacy complaint was received,<br>– The nature of the privacy complaint, and<br>– The date of the letter to the individual who made the | None |

| Categories | Privacy Indicators | OICR |
|---|---|---|
|  | privacy complaint and a brief description of the content of the letter. |  |

## Part 2 – Security Indicators

| Categories | Security Indicators | OICR |
|---|---|---|
| General Security Policies and Procedures | The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the Information and Privacy Commissioner of Ontario. | See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices (which includes reference to Appendix C). Privacy and security policies and procedures are reviewed together. |
|  | Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made. | See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices. |
|  | Whether new security policies and procedures were developed | See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices. |

| Categories | Security Indicators | OICR |
|---|---|---|
| | and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented. | |
| | The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication. | See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices. |
| | Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments. | See Part 1 – Privacy Indicators for General Privacy Policies, Procedures and Practices. |
| Physical Security | The dates of audits of agents granted approved to access the premises and locations within the premises where records of personal health information are retained since the prior review | Temporary access card audits – daily<br>Access card audits - quarterly<br>• Dec 18, 2019 (no recommendations)<br>• March 17, 2020 (no recommendations)<br>• May 27, 2020 (no recommendations) |

| Categories | Security Indicators | OICR |
|---|---|---|
|  | by the Information and Privacy Commissioner and for each audit:<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. | • Jun 18, 2020 (no recommendations)<br>• Sept 18, 2020 (no recommendations)<br>• December 15, 2020 (no recommendations)<br>• March 16, 2021 (no recommendations)<br>• July 5, 2021 (no recommendations)<br>• September 15, 2021 (no recommendations)<br>• December 15, 2021 (no recommendations)<br>• March 15, 2022 (no recommendations)<br>• June 15, 2022 (no recommendations)<br>Key audit – annually<br>• July 1, 2020 (no recommendations)<br>• November 4, 2021 (no recommendations)<br>• July 4, 2022 (no recommendations)<br>There were no recommendations arising from the audits.<br>It should be noted, however, that an audit date does not reflect the overall frequency with which OICR conducts its physical security audits. In fact, as stated herein, physical security audits are conducted daily for temporary cards, quarterly for access cards and annually for keys. Audits can also be performed as related to operational, programmatic and personnel activities. All such audits are conducted in accordance with OICR's policy and procedures on *Access Card And Key Management For Mars Location*. |
| Security Audit Program | The dates of the review of system control and audit logs since the prior review by the Information and Privacy | OTB IT audits:<br>• December 2, 2019<br>• May 19, 2020 |

| Categories | Security Indicators | OICR |
|---|---|---|
|  | Commissioner of Ontario and a general description of the findings, if any, arising from the review of system control and audit logs. | • September 8, 2020<br>• January 4, 2021<br>• February 2, 2021<br>• May 19, 2021<br>• August 24, 2021<br>• January 11, 2022<br>• January 28, 2022<br>• March 29, 2022<br>• June 9, 2022<br>(See Appendix B for descriptions) |
|  | The number and a list of security audits completed since the prior review by the Information and Privacy Commissioner of Ontario and for each audit:<br>– A description of the nature and type of audit conducted,<br>– The date of completion of the audit,<br>– A brief description of each recommendation made,<br>– The date that each recommendation was addressed | 6 OTB IT audits conducted since November 1, 2019.<br>See Appendix B for descriptions.<br>For more information: refer to OTB.POL803 *Policy and Procedures for Data Access and Use - Ontario Tumour Bank* section 5.4. |

| Categories | Security Indicators | OICR |
|---|---|---|
| | or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is expected to be addressed | |
| Information Security Breaches | The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. | Zero notifications of information security breaches or suspected information security breaches were received since the prior review by the Information and Privacy Commissioner of Ontario. |
| | With respect to each information security breach or suspected information security breach:<br>– The date that the notification was received,<br>– The extent of the information security breach or suspected<br>information security breach, | Zero notifications of information security breaches or suspected information security breaches were received. |

| Categories | Security Indicators | OICR |
|---|---|---|
|  | – The nature and extent of personal health information at issue,<br>– The date that senior management was notified,<br>– The containment measures implemented,<br>– The date(s) that the containment measures were implemented,<br>– The date(s) that notification was provided to the health information custodians or any other organizations,<br>– The date that the investigation was commenced,<br>– The date that the investigation was completed,<br>– A brief description of each recommendation made,<br>– The date each recommendation was addressed |  |

| Categories | Security Indicators | OICR |
|---|---|---|
|  | or is proposed to be addressed, and<br>– The manner in which each recommendation was addressed or is proposed to be addressed. |  |

## Part 3 – Human Resources Indicators

| Categories | Human Resources Indicator | OICR |
|---|---|---|
| Privacy Training and Awareness | The number of agents who have received and who have not received initial privacy orientation since the prior review by the Information and Privacy Commissioner of Ontario. | 5 newly hired agents (2 Collection Centre staff and 3 OICR staff) have received their initial privacy training between November 1, 2019 and August 2, 2022.<br>• November 1, 2020 - October 31, 2021: 2 Collection Centre staff and 2 OICR staff<br>• November 1, 2021 – August 2, 2022: 0 Collection Centre staff and 1 OICR staff<br>All agents having access to PHI or daily involvement with OTB have received the training.<br>Zero agents have not received initial privacy training since the prior review. |
| | The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation. | None |
| | The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by the Information and | 17 agents (9 Collection Centre staff and 8 OICR staff) have received ongoing privacy training between November 1, 2019 and August 2, 2022.<br>4 Inspirata Canada staff have signed attestations of completing ongoing privacy and security awareness training. |

| Categories | Human Resources Indicator | OICR |
|---|---|---|
|  | Privacy Commissioner of Ontario. | • November 1, 2019 – October 31, 2020: 8 Collection Center staff, 5 OICR staff and 4 Inspirata staff<br>• November 1, 2020 - October 31, 2021: 8 Collection Centre staff, 6 OICR staff and 4 Inspirata Canada staff<br>• November 1, 2021 - August 2, 2022: 5 Collection Centre staff, 6 OICR staff and 4 Inspirata Canada staff<br>Zero agents have not received ongoing privacy training since the prior review. |
|  | The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the Information and Privacy Commissioner of Ontario and a brief description of each communication. | OTB:<br>1) Annual Privacy and Information Security training is available online (online training completed in December 2019, January 2020, November 2021, December 2021 and the next training is scheduled for November 2022)<br>2) Collection Centre staff monthly teleconference (Quiz related to Privacy Policy OTB/POL801 conducted on October 21, 2020 and December 15, 2021)<br>Freezer and Operational Audit (conducted annually at each Collection Centre and at OICR) where a Privacy checklist is reviewed. See Appendix D for a copy of the Privacy checklist:<br>• February 20, 2020 – TOH<br>• February 24, 2020 – LHSC<br>• February 25, 2020 – SJH<br>• February 27, 2020 – KGH<br>• March 25, 2021 – OICR<br>• March 26, 2021 – LHSC<br>• March 29, 2021 – SJH |

| Categories | Human Resources Indicator | OICR |
|---|---|---|
|  |  | • February 17, 2022 – LHSC<br>• February 24, 2022 – SJH<br>• February 25, 2022 – KGH<br>• March 25, 2022 – OICR<br>Notes:<br>On-site access and active staff are required for these audits.<br>In 2020, OICR was due for audit in March. However, on-site access was not allowed due to COVID-19.<br>In 2021, there was no audit conducted at TOH or KGH as staff at these institutions resigned and were not replaced. There was no access to data at these sites.<br>In 2022, no audit was conducted at TOH as staff had not been replaced since their resignation in 2021. There was no access to data at the site. |
| Security Training and Awareness | The number of agents who have received and who have not received initial security orientation since the prior review by the Information and Privacy Commissioner of Ontario. | 6 newly hired agents (3 Collection Centre staff and 3 OICR staff) have received their initial security training between November 1, 2019 and August 2, 2022.<br>• November 1, 2019 -October 31, 2020: 1 Collection Centre staff and 0 OICR staff<br>• November 1, 2020- October 31, 2021: 2 Collection Centre staff and 2 OICR staff<br>• November 1, 2021- August 2, 2022: 0 Collection Centre staff and 1 OICR staff |

| Categories | Human Resources Indicator | OICR |
|---|---|---|
| | | All agents having access to PHI or daily involvement with OTB have received the training.<br>Zero agents have not received initial security training since the prior review. |
| | The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation. | None |
| | The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the Information and Privacy Commissioner of Ontario. | 17 agents (10 Collection Centre staff and 8 OICR staff) have received ongoing security training between November 1, 2019 and October 31, 2021.<br>4 Inspirata Canada staff have signed attestations of completing ongoing privacy and security awareness training.<br>• November 1, 2019 -October 31, 2020: 8 Collection Centre staff, 5 OICR staff and 4 Inspirata Canada staff<br>• November 1, 2020- October 31, 2021: 8 Collection Centre staff, 6 OICR staff and 4 Inspirata Canada staff<br>• November 1, 2021- August 2, 2022: 5 Collection Centre staff, 5 OICR staff and 4 Inspirata Canada staff<br>Zero agents have not received ongoing security training since the prior review. |

| Categories | Human Resources Indicator | OICR |
|---|---|---|
|  | The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the Information and Privacy Commissioner of Ontario. | Same as above |
| Confidentiality Agreements | The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by the Information and Privacy Commissioner of Ontario. | 7 – OICR staff signed the OICR Confidentiality Agreement.<br>10 – Collection Centre staff have signed confidentiality agreements with OTB.<br>4 – Inspirata Canada staff signed Confidentiality and Non-Disclosure Agreements with OTB.<br>All agents who have regular involvement in the program or who have access to data have signed confidentiality agreements. |
|  | The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed. | None |

| Categories | Human Resources Indicator | OICR |
|---|---|---|
| Termination or Cessation | The number of notifications received from agents since the prior review by the Information and Privacy Commissioner of Ontario related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity. | 6 agents<br>6 terminations |

## Part 4 – Organizational Indicators

| Categories | Organizational Indicators | OICR |
|---|---|---|
| Risk Management | The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the Information and Privacy Commissioner of Ontario. | The Enterprise Risk Management Committee ("Risk Management Committee") reviewed the Privacy Register as follows:<br>• January 9, 2020<br>• April 13, 2020<br>• June 15, 2020<br>• September 14, 2020<br>• November 25, 2020<br>• February 24, 2021<br>• June 9, 2021<br>• September 10, 2021<br>• November 24, 2021<br>• February 11, 2022<br>• June 7, 2022 |
| | Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made. | No amendments |
| Business Continuity and Disaster Recovery | The dates that the business continuity and disaster recovery plan was tested since the prior review by the Information and | Business Continuity and Disaster Recovery testing of this plan was completed on July 26, 2022. |

| | | |
|---|---|---|
| | Privacy Commissioner of Ontario. | |
| | Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made. | No amendments |

## Appendix A: Privacy Recommendations from the OTB's annual Freezer and Operational Audit

| Date of Audit | Recommendation | Date Addressed | Response |
|---|---|---|---|
| February 24, 2022 | SJH: Passwords must not contain any words that can be found in the dictionary, even if they are accompanied by numbers and other letters within a user password. | April 5, 2022 | Password updated by user immediately after notification. |

## Appendix B: Ontario Tumour Bank Security IT Audit Summary

| | Type of Audit | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Audit Date | OICR VPN Access[1] | R Drive Access[2] | OTB Inbox Access[3] | TMx – Application[4] | TMx – Oracle[5] | OTB Scan Folder[6] | SSLVPN (Inspirata Canada access)[7] | OTB SharePoint[8] |
| December 2, 2019 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |
| May 19, 2020 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |
| September 8, 2020 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |
| January 4, 2021 | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator | No recommendations made.<br>**Removed:** Client Coordinator |

|  | Type of Audit |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Audit Date | OICR VPN Access[1] | R Drive Access[2] | OTB Inbox Access[3] | TMx – Application[4] | TMx – Oracle[5] | OTB Scan Folder[6] | SSLVPN (Inspirata Canada access)[7] | OTB SharePoint[8] |
| February 2, 2021 | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Added:** Client Coordinator<br>**Removed:** Clinical Research Coordinator |
| May 19, 2021 | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator | No recommendations made.<br>**Removed:** Clinical Research Coordinator |
| August 24, 2021 | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead | No recommendations made.<br>**Added:** Project Lead |

| Audit Date | Type of Audit | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | OICR VPN Access[1] | R Drive Access[2] | OTB Inbox Access[3] | TMx – Application[4] | TMx – Oracle[5] | OTB Scan Folder[6] | SSLVPN (Inspirata Canada access)[7] | OTB SharePoint[8] |
| November 11, 2021 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |
| December 23, 2021 | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst | No recommendations made.<br>**Removed:** Data Analyst |
| January 28, 2022 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |
| March 29, 2022 | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director | No recommendations made.<br>**Added:** Data Analyst<br>**Removed:** Director |

|  | Type of Audit |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Audit Date | OICR VPN Access[1] | R Drive Access[2] | OTB Inbox Access[3] | TMx – Application[4] | TMx – Oracle[5] | OTB Scan Folder[6] | SSLVPN (Inspirata Canada access)[7] | OTB SharePoint[8] |
| June 6, 2022 | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. | No recommendations made. |

[1] Audits users that currently have access to OICR's VPN

[2] Audits users who have access to the OTB folder on FS10: R:\H-Tumour Bank

[3] Audits active users who have access to the shared OTB Inbox on Exchange

[4] Audits (i) active TissueMetrix Accounts in Production; (ii) Audit TissueMetrix account login

[5] Audits list of users with Oracle Production DB Accounts

[6] Audits read/write access to the OTB scan folder

[7] Audits: shell account logs (username, date/time logged in, date/time logged off)

[8] Audits: (i) owners of all OTB program files; (ii) OTB SharePoint user groups; and (iii) OTB Collaboration access

# Appendix C: OICR Policy Reviews and Amendments

Please Note: all approved policies are communicated by posting the policy on the OICR intranet immediately after approval.

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| Access Card and Key Management for MaRS Location | Log of Access to OICR Premises—OICR Access Cards (F-AD-SEC.504-01); Log of Access to OICR Premises—OICR Keys (F-AD-SEC.504-02); Day Pass Access Card Log (F-AD-SEC.504-03); MaRS Access Cards Request Form for OICR (F-AD-SEC.504-04); MaRS Key Request form (F-AD-SEC.504-05); MaRS Authorization to Issue Transfer Key (F-AD-SEC.504-06); OICR Incident Report Form (F-AD-SEC.502-03) | AD-SEC.504.003 | Administrative—Facilities Security | Senior Manager, Facilities | Senior Manager, Facilities; Vice President Corporate Services and Chief Financial Officer | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 10-Mar-2021 | |
| Clean Desk Policy | | AD-GEN.104.003 | Administrative—General Administration and Risk Management | Vice President, Corporate Services and Chief Financial Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 11-Dec-2020 | |
| Confidentiality of Information | Log of Confidentiality Agreements (F-PR-INS.102-01); OICR Confidentiality Agreement (F-PR-INS.102-02) | PR-INS.102.002 | Privacy and Information Security – Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-Jun-22 | |
| Data Use and Disclosure Policy | Project Privacy Evaluation Form (F-PR-INS.201-01) | PR-INS.201.004 | Privacy & Information Security—Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-Jun-22 | |
| Policy on the Development and Management of Policies | Policy Template | AD-GEN.101.006 | General Administration and Risk Management | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 14-Sep-21 | 18-Aug-21 | **AD-GEN.101.006**<br>Approved and communicated 14-Sep-21<br>• Policy Template replaced previous forms named:<br>o Template for Development of Policies and Procedures (F-AD-GEN.101-01)<br>o Approval / Change Request Form for Policies, Procedures and Guidelines (F-AD-GEN.101-02)<br>• "Development and Management of Policies, Procedures and Guidelines" was superseded by this policy. It fulfills the same purpose with updated language and detail on clerical tasks required. |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| Execution of Data Sharing Agreements | Data Sharing Agreement Log (F-PR-INS.205-01), Data Sharing Agreement Template (F-PR-INS.205-02) | PR-INS.205.002 | Privacy and Information Security – Privacy – Data Management | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-Jun-22 | |
| Execution of Third Party Service Provider Agreements | Third Party Service Provider Agreement (Template) (F-AD-GEN.105-01), Log of Third Party Service Agreements (F-AD-GEN.105-02) | AD-GEN.105.002 | Administration—General Administration and Risk Management | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-Jun-22 | |
| Facilities Security Policy | Visitor Log (F-AD-SEC.502-01); Day Pass Access Card Log (F-AD-SEC.504-03); Lost and Found Log (F-AD-SEC.502-02); OICR Incident Report Form (F-AD-SEC.502-03) | AD-SEC.502.005 | Administrative—Facilities Security | Senior Manager, Facilities | Senior Manager, Facilities | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 9-Feb-2021 | |
| General Breach Report / Investigation Form | | F-PR-INS.301-01 | Privacy & Information Security--Privacy | | Privacy Officer | | | | 28-Jun-22 | |
| Glossary for Privacy Policies and Procedures | | D-PR-INS.103 | Privacy & Information Security–Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 26-Aug-2020 | |
| Investigation and Reporting of Suspected Theft for MaRS Location | OICR Incident Report Form (F-AD-SEC.502-03) | AD-SEC.506.003 | Administrative—Facilities Security | Senior Manager, Facilities | Senior Manager, Facilities | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 9-Mar-21<br>15-Mar-2022 | |
| OICR Corporate Risk Management Policy | | AD-GEN.106.003 | General Administration and Risk Management | Vice President, Corporate Services and Chief Financial Officer | Corporate Secretary; Vice President, Corporate Services and Chief Financial Officer; Corporate Management and Executive Management | Vice President, Corporate Services and Chief Financial Officer and Risk and Compliance Manager | Board of Directors | 25-Jun-20 | 15-May-20 | AD-GEN.106.003<br>Approved and communicated 25-Jun-20<br>• Removal of Section 4.3 Risk Appetite |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| OICR Incident Report Form | Facilities Security; Investigation and Reporting of Facilities Security Incidents; Accident Reporting and Investigation | F-AD-SEC.502-03 | Administration—Facilities Management; Health and Safety | Senior Manager, Facilities; Health and Safety Officer | Senior Manager, Facilities; Health and Safety Officer | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 10-Mar-2021 | |
| Ontario Institute for Cancer Research (OICR) Information Security Program | | PR-INS.800.006 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-2020 | 21-Apr-2020 | PR-INS.800.006<br>Approved and communicated 16-Jul-20<br>• Copy edits<br>• Discretionary power of Information Security Officer to intervene when threat added in Section 2.0<br>• Emphasis on security added in Section 5.0<br>• Added cloud based infrastructure or service in Section 7.0<br>• Removed Technical Ease section<br>• Replaced ISO with ITHelpdesk for who to contact<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy<br>• Updated the policy title to "Ontario Institute for Cancer Research (OICR) Information Security Program" |
| OICR Privacy and Information Security Accountability Terms of Reference | | PR-INS.103.002 | Privacy and Information Security – General Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 28-June-22 | |
| OICR Privacy Policy | | PR-INS.101.005 | Privacy & Information Security--Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 28-June-22 | |
| Personal Information Guideline | | No policy number as this is a guideline. | Privacy and Information Security—OICR Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 28-June-22 | |
| Policies and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information | | PR-INS.206.002 | Privacy & Information Security -- Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| Policy and Procedures for Maintaining a Consolidated Log of Recommendations | OICR's Consolidated Log of Privacy and Information Security Recommendations (F-PR-INS.104-01) | PR-INS.104.002 | Privacy & Information Security—General Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| Policy and Procedures for Information Security and Privacy Breach Management | Breach Investigation Form (F-PR-INS.301-01), Log of Privacy Breaches (F-PR-INS.301-02) | PR-INS.301.001 | Privacy & Information Security—Privacy – Breach Management | Privacy Officer and Information Security Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| Policy and Procedures in Respect of a Security and a Privacy Audit | Privacy Audit Report Template (F-PR-INS.204-01), Privacy Audit Log (F-PR-INS.204-02) | PR-INS.204.001 | Privacy & Information Security—Data Management | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| 01.0 Acceptable Use | | AD-INT.201.005 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 17-Apr-20 | AD-INT.201.005<br>Approved and communicated 11-Jun-20<br>• Added cloud services to scope of policy<br>• Modification of procedure under section 2.1 – using email to request support from helpdesk instead of a ticket system<br>• Added that this policy applies regardless of physical location – applies when working from home<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 11.0 IT Risk Assessment Policy and Threat Risk Assessment Guide | | PR-INS.811.003 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-20 | 22-Apr-20 | PR-INS.811.003<br>Approved and communicated 16-Jul-20<br>• Copy-edit<br>• Obligation to perform a Vulnerability Assessment has been introduced under section 1<br>• Changes to roles and accountabilities in Section 3<br>• Annual TRA instead of every other year<br>• Clarified targets<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 12.0 Change Controls (OICR Production Servers) | | PR-INS.812.005 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-20 | 17-Apr-20 | PR-INS.812.005<br>Approved and communicated 16-Jul-20<br>• Increased annual global maintenance windows to four<br>• Clarified requirements of test plans<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 13.0 Server Security | | PR-INS.813.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jul-20 | 6-May-20 | PR-INS.813.004<br>Approved and communicated 11-Jul-20<br>• Added procedure in Section 3.1 to conduct Vulnerability Scan and ensure Critical or High vulnerabilities are mitigated<br>• Copy editing<br>• Removed statement that admin does not have remote access<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Security Officer was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 14.0 Network Security | | PR-INS.814.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 7-Aug-20 | PR-INS.814.004<br>Approved and communicated 10-Sep-20<br>• New standards in Section 2 have been added including regarding VLANS, TCP/IP, IEEE 802.1x, and Wi-Fi Protected Access (WPA2) enterprise Protection Extensible Authentication Protocol (PEAP) |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • Added procedure in Section 3 stating that network should be created in a principle of least privilege manner i.e. access to and from the network granted to the service(s) required for the defined scope<br>• Section 2.5: Added IEEE 802.1x<br>• Section 2.7: Added Secure SSL Gateway (Portico)<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 15.0 Workstation Security | | AD-INT.215.004 | Administrative--Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 6-May-20 | AD-INT.215.004<br>Approved and communicated 11-Jun-20<br>• Copy edit – changed case on one letter<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 16.0 Personal Use of the Ontario Institute for Cancer Research's Systems | | AD-INT.216.005 | Administrative–Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 5-Aug-20 | AD-INT.216.005<br>Approved and communicated 10-Sep-20<br>• Removed Trojan horses in Section 2<br>• Added text regarding interfering with any OICR employee and that OICR cannot guarantee return, integrity or retention of personal data<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy<br>• Updated the policy title to "Personal Use of the Ontario Institute for Cancer Research's Systems" |
| 17.0 Personal/Third Party Devices Interacting with OICR Systems | | AD-INT.217.004 | Administrative–Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 7-Aug -20 | AD-INT.217.004<br>Approved and communicated 10-Sep-20<br>• New statement establishing that access to OICR's secure internal networks will be provided to OICR owned and managed devices only<br>• Updated Section 2 to state that non-OICR devices can access internet and OICR email but are prohibited for access or storage of Level 4 data<br>• Added language around use of non-OICR devices for offsite access<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 18.0 Electronic Mail Security | | AD-INT.218.006 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Nov-20 | 20-Apr-20<br>22-Oct-2020 | AD-INT.218.006<br>Approved and communicated 10-Nov-20<br>• Weekly SPAM Report can be requested via the OICR Helpdesk<br>• Added statement about phishing email<br>• Corrected statements about OWA and mail filtering<br>• Removed section on Exceptions<br>• Added a statement about OICR IT invoking auto-archiving (where messages greater than 1 year old are automatically moved to an Archive folder, but are still accessible via Outlook or Webmail) in Section 2.9<br>• Added that OICR email can be accessed through an OICR managed BYOD application<br>• Removed the Related Documents section from the policy<br>• Copy edits<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  | • Corporate Management was replaced by Executive Management as the approver of the policy |
| 19.0 Extranet Security |  | PR-INS.819.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 21-Apr-20 | PR-INS.819.004<br>Approved and communicated 11-Jun-20<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 02.0 Data Classification |  | PR-INS.802.005 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 17-Apr-20 | PR-INS.802.005<br>Approved and communicated 11-Jun-20<br>• Copy edits<br>• Replaced ISO and Privacy Officer with IGC<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 20.0 Anti-Virus Administration |  | PR-INS.820.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 17-Apr-20 | PR-INS.820.004<br>Approved and communicated 11-Jun-20<br>• Updated definitions of antivirus<br>• Removed obsolete language<br>• Removed involvement of Corporate IT Security Lead and Symantec<br>• Monitor for zero day<br>• Minimum of weekly scheduled scans<br>• The sponsor's title was updated from Privacy & Information Security – IT Information Security to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 22.0 Remote Access |  | PR-INS.822.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 13-Aug-20 | 14-Jul-20 | PR-INS.822.004<br>Approved and communicated 13-Aug-20<br>• Added warning in section 2.7 on use of open Wi-Fi<br>• Removal of Section 1.1 with regards to risk definitions for readability purposes<br>• Single factor authentication or preferably two-factor authentication provides remote access to users<br>• Approved users may be granted access to their OICR based computer using a secure remote desktop access technology in Section 2.1.2<br>• Updated the usage of single factor and two factor authentication in Section 2.12 and 2.13<br>• Copy edits<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Security Officer was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • Vice President, Corporate Services and Chief Financial Officer was replaced by Executive Management as the approver of the policy |
| 23.0 Electronic Media Destruction | | PR-INS.823.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Nov-20 | 20-Apr-20<br>20-Oct-20 | PR-INS.823.004<br>Approved and communicated 10-Nov-20<br>• Added statements that data backed up using encrypted backup jobs through Commvault can be securely destroyed by purging the encryption key without needing to remove the actual encrypted data<br>• Removed "Related Documents" section from the policy<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 24.0 Declaration and Disposal of Surplus IT Equipment | | PR-INS.824.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 20-Apr-20 | PR-INS.824.004<br>Approved and communicated 11-Jun-20<br>• Copy edits<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 25.0 IT HelpDesk Services Security | | PR-INS.825.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 21-Apr-20 | PR-INS.825.004<br>Approved and communicated 11-Jun-20<br>• Password reset, temp password<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 26.0 Employees on Temporary (Short or Long-Term) Leave | | AD-INT.226.005 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer; Director, Human Resources | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 13-Aug-20 | 14-Jul-20 | AD-INT.226.005<br>Approved and communicated 13-Aug-20<br>• Updated Section 1 to state that managers must also take precautions to ensure that their employee's absence does not create vulnerabilities to the security of OICR's information assets<br>• Changes to short- and long-term leave procedures<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 27.0 Employees Departing OICR | | AD-INT.227.004 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-20 | 20-Apr-20 | AD-INT.227.004<br>Approved and communicated 16-Jul-20<br>• Managers can request access to email of departed employees pursuant to s. 3.7<br>• Mobile device, retain number<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| 28.0 Mobile Devices Security |  | AD-INT.228.006 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-2020 | 24-Apr-20<br>4-Aug-20 | AD-INT.228.006<br>Approved and communicated 10-Sep-20<br>• Added that use of App or integration with a third party cloud service must be compliant with policy and removed prohibition of third party sync services or cloud for data management in Section 2.1<br>• Removed prohibition to use App for data management in Section 2.5<br>• Added face recognition/biometric and/or PIN to unlock<br>• Changed PIN from min 4 characters to 6<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 29.0 Disaster Recovery and Offsite Data Storage |  | PR-INS 829.004 | Privacy & Information Security—IT Information Security | Senior Director, IT / Information Security Officer | Senior Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 8-Apr-21 | 19-May-20<br>17-Feb-21 | PR-INS.829.004<br>Approved and communicated 8-Apr-21<br>• Added secure cloud based backups<br>• Updated policy statement to state that OICR will enhance tape backups with secure cloud based backups where cloud based backup solution offers acceptable and equivalent security compared to magnetic tape<br>• Updated in Section 2.1 that data (identified by data owner) that needs to be backed up to tape is kept onsite at OICR for 2-6 weeks<br>• Updated in Section 2.4 that the systems can run for up to several days/weeks<br>• Updated Section 2.3 regarding Financial data<br>• Added Manager, Corporate Systems as a testing supervisor in Section 2.3<br>• Updated Data Storage Procedures in Section 3.1<br>• Updated that the disaster recovery standards and procedures are reviewed and tested on an as-requested basis by the Data Owner<br>• Updated that the testing of backup and recovery of records related to the OTB must occur annually<br>• Removed Related Document section from the policy<br>• Updated job titles<br>• Copy edits<br>• Removed requirement for dedicated tapes for Level 4 PHI backups<br>• Added description of how backup job level encryption provides safeguards<br>• The sponsor's title was updated to Senior Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Senior Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 03.0 Encryption |  | PR-INS.803.005 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 4-Aug-20 | PR-INS.803.005<br>Approved and communicated 10-Sep-20<br>• Changes to encryption standards for removal media with Level three and Level four data<br>• Copy edits<br>• Updated the purpose of the policy to state the importance of strong encryption in Section 1<br>• Added Section 2.8 to state the importance of software or hardware encryption of tapes<br>• Updated Section 3.2 on the use of removable media storing data classified as Level Three.<br>• In some cases the Information Security Officer may approve the use of removable media procured or provided by a collaborator<br>• In all cases, the decryption password/passphrases/keys must be communicated out of band using a tool like OICR Whisper<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee and Information Security Officer were replaced by Director, IT/ Information Security Officer as the content reviewer of the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • Corporate Management was replaced by Executive Management as the approver of the policy |
| 30.0 Research Lab Security | | PR-INS.830.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 7-Aug-20 | PR-INS.830.004<br>Approved and communicated 10-Sep-20<br>• Added a procedure where if any USB media of unknown origin has been found, it must not be inserted into a computer and IT Helpdesk should be informed in Section 3.4<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 31.0 Loaner Devices | | AD-INT.231.004 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 04-Aug-20 | AD-INT.231.004<br>Approved and communicated 10-Sep-20<br>• Added requirements in Sections 3.2 and 3 3<br>• Added statement that ERT can extend 2 week period<br>• Copy editing<br>• Defined Loaner as laptop or mobile device<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 32.0 Restricted or Non-Networked Computing Environments | | PR-INS.832.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 7-Aug-20 | PR-INS.832.004<br>Approved and communicated 10-Sep-20<br>• Added clarifications to statement<br>• Prohibition to receive inbound connections in Section 2.1<br>• Changes in Section 2.2 include "must be" instead of "are" and "ensure traffic is isolated from the rest of the OICR network"<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 33.0 Patch Management | | PR-INS.833.006 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 10-Sep-20 | 4-Aug-20 | •<br>PR-INS.833.006<br>Approved and communicated 10-Sep-20<br>• Copy editing<br>• Update terminology to include OpenStack, SCCM<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 36.0 Mobile Device Allocation | | AD-INT.236.006 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 24-Apr-20 | AD-INT.236.006<br>Approved and communicated 11-Jun-20<br>• Removed reference to Blackberry<br>• Added face recognition to unlock device<br>• Added details around purchasing device or transferring phone number upon termination<br>• Clarified that employees must keep their mobile devices secure<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • Corporate Management was replaced by Executive Management as the approver of the policy |
| 38.0 IT Device (Hardware and Software) Allocations | Mobile Devices User Agreement (F-AD-INT.238-01) | AD-INT.238.003 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-20 | 23-Apr-20 | **AD-INT.238.003**<br>Approved and communicated 16-Jul-20<br>• Copy edit<br>• Device considered high risk after 5 years in Section 3.2<br>• Increased threshold to 5 years in Section 4.3<br>• Thresholds changed in Table 1, 3 and 4<br>• Increased recommended limit for Tier 3 Research computer cost<br>• Added language to suggest laptop use<br>• Copy editing to clarify points in Section 3.2, 3.3 and 3.5.1<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• Director, Finance was removed as a sponsor of the policy<br>• The Manager, Procurement was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Vice President Corporate Services and Chief Financial Officer as the issuer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 04.0 Secure Electronic Data Retention, Backup, Disposal and Destruction | | PR-INS.804.005 | Privacy & Information Security—IT Information Security | Senior Director, IT / Information Security Officer | Senior Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 8-Apr-21 | 1-Mar-21 | **PR-INS.804.005**<br>Approved and communicated 8-Apr-21<br>• Changes to Statement in Section 2 with reference to cloud services<br>• The default point in time back up schedule cycle and retention has been updated to primarily state the maximum retention of back ups is one year<br>• Added that data owners can request for longer retention or different schedules<br>• Added secure data deletion methods<br>• Deleted references to backup in section 5<br>• Removal of the Related Documents Section of the policy<br>• Updated policy titles and job titles<br>• Copy edits<br>• The sponsor's title was updated to Senior Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Senior Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 05.0 Data Protection (Encryption, Transmission and Storage) | | PR-INS.805.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 16-Jul-20 | 17-Apr-20<br>19-May-20 | **PR-INS.805.004**<br>Approved 16-Jul-20<br>• Updated terminology<br>• Updates to encourage encryption for any level in transit<br>• Added requirement for encrypted backups for Level 3<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 06.0 Access Control, Identification and Authentication | | PR-INS.806.005 | Information Technology & Information Security | Senior Director, IT / Information Security Officer | Senior Director, IT / Information Security Officer | Senior Vice-President, Group Chief Financial Officer | Executive Management | 11-Jun-20<br>10-Mar-22 | 12-May-20<br>02-Mar-22 | **PR-INS.806.004**<br>Approved and communicated 11-Jun-20<br>• Replaced stakeholder with user<br>• Services to include onsite and in the cloud<br>• Added requirement for two factor authentication for cloud based services<br>• Corporate Management was replaced by Executive Management as the approver of the policy<br>**PR-INS.806.005**<br>Approved and communicated 10-Mar-22<br>• Added a 'Scope' to the policy |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • Added the definitions of 'Application Owner', 'Users' and 'OICR Individuals' to the policy<br>• Added that Multi Factor/Two-factor authentication is mandatory for any internet accessible user account in Section 1.0<br>• Added when and by whom user accounts are created or amended in Section 1.0<br>• Removal of the 'Procedure' Section<br>• Removal of the 'Related Documents' Section<br>• Copy edits<br>• The sponsor's title was updated to Senior Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Senior Director, IT/ Information Security Officer as the content reviewer of the policy<br>• The issuer's title was updated to Senior Vice-President, Group Chief Financial Officer<br>• Privacy & Information Security—IT Information Security was updated to Information Technology & Information Security |
| 07.0 Password Governance | | AD-INT.207.005 | Information Technology & Information Security | Senior Director, IT / Information Security Officer | Senior Director, IT / Information Security Officer | Senior Vice-President, Group Chief Financial Officer | Executive Management | 13-Aug-20<br>10-Mar-22 | 29-Apr-20<br>02-Mar-22 | **AD.INT.207.004**<br>Approved and communicated 13-Aug-20<br>• Application of policy to assets on site and cloud<br>• New password storage and protection requirements in Section 2.2<br>• Copy editing<br>• Added that private keys must be password protected<br>• Corporate Management was replaced by Executive Management as the approver of the policy<br>**AD.INT.207.005**<br>Approved and communicated 10-Mar-22<br>• Added a 'Scope' to the policy<br>• Added the definitions of 'Application Owner', 'Users' and 'OICR Individuals' to the policy<br>• Amended that passwords for all levels of access requiring authentication must contain a minimum of twelve (12) characters<br>• Added Section 4.2.2 regarding 'Password Storage and Protection Recommendations' to the policy<br>• Amended Section 4.3 regarding 'Password expiry'<br>• Added mandatory standards such as 'Multi Factor Authentication/Two-Factor Authentication', 'Microsoft Passwordless Authentication', User Self Service Password Reset'<br>• Amended the 'Procedures' in Section 7.0<br>• The review and approval period of this policy has been increased to three (3) years<br>• Removal of the 'Related Documents' Section<br>• Copy edits<br>• The sponsor's title was updated to Senior Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Senior Director, IT/ Information Security Officer as the content reviewer of the policy<br>• The issuer's title was updated to Senior Vice-President, Group Chief Financial Officer<br>• Administrative - Information Security was updated to Information Technology & Information Security |
| 08.0 Internet Usage | | AD-INT.208.006 | Administrative—Information Technology | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 21-Apr-20 | **AD-INT.208.006**<br>Approved and communicated 11-Jun-20<br>• Change to policy statement – must adhere to all OICR policies and not just to the Acceptable Use policy<br>• Added in the policy statement the right for OICR to log all communications technologies<br>• Added section on caution with email links and attachments<br>• Personal use must be incidental<br>• The sponsor's title was updated to Director, IT/ Information Security Officer |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | • The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| 09.0 Access to OICR Systems by Contractors, Consultants & Third Parties | | PR-INS.809.004 | Privacy & Information Security—IT Information Security | Director, IT / Information Security Officer | Director, IT / Information Security Officer | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 11-Jun-20 | 17-Apr-20 | PR-INS.809.004<br>Approved and communicated 11-Jun-20<br>• Added application of policy to remote access<br>• The sponsor's title was updated to Director, IT/ Information Security Officer<br>• The Information Governance Committee was replaced by Director, IT/ Information Security Officer as the content reviewer of the policy<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| Privacy and Information Security Training and Awareness Policy | Privacy and Information Security Attestation (F-PR-INS.601-01); Privacy and Information Security Attestation—Specialized Role-Based Training for Ontario Tumour Bank (F-PR-INS.601-02); Log of Privacy and Information Security Training (L-PR-INS.601-03) | PR-INS.601.003 | Privacy & Information Security—Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| Privacy Complaint Policy and Procedures | Privacy Complaint Log (F-PR-INS.702-01) | PR-INS.702.004 | Privacy & Information Security—Privacy — Privacy Information for the Public | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| Privacy Impact Assessment Policy | Log of Privacy PIA (F-PR-INS.501-01) | PR-INS.501.002 | Privacy & Information Security—Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 27-June-22 | |
| Privacy Inquiry Policy and Procedures | Log of Privacy Inquiries (F-PR-INS.701-01) | PR-INS.701.004 | Privacy & Information Security—Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management | | 28-June-22 | |
| Progressive Discipline Policy | | AD-HRE.612.004 | Administrative – Human Resources – Employment | Director, Human Resources | Corporate Management | Vice President, Corporate Services and Chief Financial Officer | Executive Management | 8-Jul-21 | 14-Jun-21 | AD-HRE.612.004<br>Approved and communicated 8-Jul-21<br>• Updated the definition of 'Paid Suspension' and 'Written Warning'<br>• Copy edits to the purpose, the scope and the definitions of 'Employee' and 'Verbal Warning'<br>• Added that investigations may include a review of video or other OICR-managed technologies in Section 5.1<br>• Formatting and copy edits |

| Policy Title | Associated Form(s) | Policy Number | Section | Sponsor | Content Reviewer(s) | Issued By | Approved By | Last Modified | Review Dates | Revision Comments |
|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  | • Grammatical changes<br>• Updated policy titles<br>• Corporate Management was replaced by Executive Management as the approver of the policy |
| Retention and Disposal of Administrative Records |  | PR-INS.203.003 | Privacy & Information Security—Data Management | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management |  | 27-June-22 |  |
| Retention, Transfer and Disposal of Records Containing Personal Information, Personal Health Information and De-identified Health Information |  | PR-I NS.202.004 | Privacy & Information Security—Data Management | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management |  | 28-June-22 |  |
| Sending / Receiving Personal Information, Personal Health Information and De-Identified Health Information |  | PR-INS.401.003 | Privacy & Information Security–Privacy | Privacy Officer | Information Governance Committee | Vice President, Corporate Services and Chief Financial Officer | Corporate Management |  | 29-June-22 |  |
| Termination Policy |  | AD-HRE.611.005 | Administrative – Human Resources – Employment | Director, Human Resources | Corporate Management | Vice President, Corporate Services and Chief Financial Officer | Executive Committee | 9-Mar-20 | 12-Feb-20 | AD-HRE.611.005<br>Approved and communicated 9-Mar-20<br>• Updated format and procedural details<br>• Added 4.1 repayment of vacation taken but not accrued<br>• Modified 4.2 regarding access to OICR data<br>• Added 4.5 Access to Terminated Employee's Email and statement about personal data ownership<br>• Added related documents<br>• Removed language in compliance section<br>• Corporate Management was replaced by Executive Committee as the approver of the policy<br>• Removed associated forms as these are now procedural documents |

## Appendix D: OTB Privacy Checklist

The following is an excerpt from *F-QA604-01 – Collection Centre Freezer and Operational Audit Agenda* under Section 5. Privacy & Information Security.

### 5. PRIVACY & INFORMATION SECURITY

| | **Staff 1** | **Staff 2** |
|---|---|---|
| Have both CC staff completed OICR privacy and information security training within the past year?<br>When? | | |
| When do you log out of TissueMetrix?<br>Do you lock your workstation when you leave?<br>Does your screensaver lock automatically with a required password to unlock? (check screensaver setting and report lockout time)<br>Does anyone else (OTB or other) have access to your workstation? | | |
| Do you share your password?<br>Do you write down or store your passwords anywhere?<br>Do you use known words, *etc.*? | | |
| Do you email screenshots (*i.e.*, to Inspirata or OICR for troubleshooting)?<br>What method do you use to take screenshot?<br>Do you review the screenshot to ensure it does not have any patient identifying information?<br>How do you edit the image to remove PHI? | | |
| Do you use a USB key or laptop?<br>If yes, are they encrypted? | | |
| Can you provide a hypothetical example of a privacy or information security breach? | | |

| | | |
|---|---|---|
| What would you do? | | |
| Have there been any privacy/information security breaches within the last year?<br>Were they reported?<br>To whom? | | |
| Are consent forms kept in a locked cabinet?<br>If yes, who has keys? | | |
| Who has access to the sample storage equipment (*i.e.*, freezer, slide and block cabinets, dry shippers)?<br>Are they locked?<br>If yes, who has keys? | | |
| What other paper documents are retained for the program?<br>Do any contain patient (identifying) information and why is it necessary?<br>Are any printed from TM?<br>How are the documents stored, for how long, and who has access? | | |
| What other electronic files (*i.e.*, spreadsheets) are maintained for the program?<br>Do any contain patient (identifying) information and why is it necessary?<br>Where are the files stored and who can access them (*i.e.*, secure drive)? | | |
| Is any information circulated to other groups (*i.e.*, LMC or surgeons)?<br>Describe the detail included. | | |
| Where is your confidential waste bin (for shredding) is located? | | |

| | |
|---|---|
| Do you ever place lists/TM printouts within recycling? | |

**Additional Comments:**

Click here to enter text.